HOUSE OF REPRESENTATIVES STAFF ANALYSIS

BILL #: HB 343 Payment Card Offenses
SPONSOR(S): Asencio
TIED BILLS: **IDEN./SIM. BILLS:** SB 766

REFERENCE	ACTION	ANALYST	STAFF DIRECTOR or BUDGET/POLICY CHIEF
1) Criminal Justice Subcommittee		Merlin	White
2) Justice Appropriations Subcommittee			
3) Judiciary Committee			

SUMMARY ANALYSIS

As in most states, Florida has laws to protect citizens from credit card or payment card "skimming," which involves obtaining private information from a card used in an otherwise normal transaction.

According to the National Conference of State Legislatures, more than half of the states have enacted some form of anti-skimming legislation aimed at fraudulent use of electronic scanning devices and reencoders which can be used to store encoded payment information or transfer the data to another card. No state, however, prevents outright ownership of such devices or creates any presumptions regarding their possession.

In Florida, section 817.625, F.S., provides that it is a felony of the third degree to use a scanning device or reencoder without the permission of the authorized card user, and with the intent to defraud the authorized user, the issuer of the authorized user's payment card, or a merchant. A second or subsequent violation of the statute is a felony of the second degree. Any person who violates the statute is subject to civil forfeiture.

At present, section 817.625, F.S., does not address payment cards with computer chips, nor does it address possession of a scanning device or create any presumptions regarding possession or intent to defraud.

The bill expands the current definitions of "reencoder" and "scanning device" to include a "computer chip" or other storage mechanism, or from another device that directly reads the information from the card. The bill also:

- Creates a new third degree felony offense that prohibits a person from possessing, selling, or delivering a scanning device knowingly and with the intent to defraud an authorized user of a payment card, the issuer of a payment card, or a merchant; and
- Provides that it is prima facie evidence of a person's knowledge and intent to defraud if the person possessing the scanning device is not a law enforcement officer or other similar individual specified in the bill.

The Criminal Justice Impact Conference ("CJIC") considered this bill on March 2, 2017, and determined that it will have a positive insignificant impact on prison beds, meaning an increase of ten or fewer prison beds. Please see "FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT," *infra.*

The bill provides an effective date of October 1, 2017.

FULL ANALYSIS

I. SUBSTANTIVE ANALYSIS

A. EFFECT OF PROPOSED CHANGES:

Overview of Skimming: Use of Devices to Obtain Protected Payment Card Information

As in most states, Florida has laws to protect citizens who use credit cards and other similar payment cards against fraudulent practices. A "payment card" is a "credit card, charge card, debit card, or any other card that is issued to an authorized card user and that allows the user to obtain, purchase, or receive goods, services, money, or anything else of value from a merchant."[1]

In recent years, state and local law enforcement agencies ("LEA's") have reported on the practice of "skimming," which involves obtaining private information from someone's payment card used in an otherwise normal transaction such as at an ATM.[2] A criminal suspect can obtain a victim's card number by photocopying receipts, copying a PIN code, or using an electronic scanning device[3] or reencoder[4] to swipe and store a victims' payment card numbers or transfer the data or information to another card.[5] Skimming can occur at a restaurant or bar where the skimmer has possession of the victim's card out of their immediate view.[6] Similarly, skimming can also occur at gas stations when a third-party card-reading device is installed either outside or inside a fuel dispenser[7] or other card-swiping terminal.[8]

In Florida, the Department of Agriculture and Consumer Services ("DACS") is the state agency that is responsible for collecting samples and testing fuel quality at gas station pumps and dispensers and making sure that such dispensers are working properly.[9] The authority to investigate and enforce criminal laws regulating such businesses and the security of consumers is governed by the Office of Agricultural Law Enforcement ("AGLAW").[10] DACS has reported that AGLAW typically comes across skimming devices during fuel theft or gas skimming investigations.[11]

---

[1] s. 817.625(1)(c), F.S.; *see also* s. 817.615(1)(d), F.S. (defining a "merchant" as "a person who receives from an authorized user of a payment card, or someone the person believes to be an authorized user, a payment card or information from a payment card, or what the person believes to be a payment card or information from a payment card, as the instrument for obtaining, purchasing, or receiving goods, services, money, or anything else of value from the person.").

[2] Article, *"Taking a Trip to the ATM? Beware of Skimmers,"* Federal Bureau of Investigation ("FBI") (July 14, 2011), *available at* https://www.fbi.gov/news/stories/atm-skimming (last viewed Feb. 3, 2017); *see also Arnauta v. State*, 125 So. 3d 1028, 1029 (Fla. 4th DCA 2013) (noting, in part, that charges were filed against the defendant after police discovered that the defendant had used an ATM skimming device to withdraw money from customer accounts and after police searched the defendant's residence, storage units and vehicle, discovering a multitude of ATM parts, molds, ATM keypads, circuit boards, blank bank credit cards, magnetic strips, and bank card readers/writers. At trial, Citibank employees testified 171 accounts had to be closed and re-opened as customers used their cards during the period when the ATM machines were compromised. Money was removed from thirty-one accounts, with the loss to Citibank totaling more than $44,000 plus the cost of closing and re-opening the accounts.).

[3] s. 817.625(1)(a), F.S.

[4] s. 817.625(1)(b), F.S.

[5] Feinberg, Ashley, *"The Evolution of ATM Skimmers,"* Gizmodo (Aug. 27, 2014), *available at* http://gizmodo.com/the-terrifying-evolution-of-atm-skimmers-1626794130 (last viewed Feb. 3, 2017).

[6] Denny, Dawn, *"Cashier Linked to Credit Card Skimming Scam, Police Say*," KXAN (May 20, 2014), *available at* http://kxan.com/2014/05/20/restaurant-cashier-linked-to-credit-card-skimming-scam-police-say/ (last viewed Feb. 3, 2017).

[7] Jacobson, Susan, *"State Finds 103 Credit-Card Skimmers in 3-month Inspection of Gas Pumps,"* ORLANDO SENTINEL (May 19, 2015), *available at* http://www.orlandosentinel.com/business/os-gas-pump-skimmers-20150519-story.html (last visited Feb. 4, 2017).

[8] Musil, Steven, *"13 Indicted in $2M Gas Station Card-Skimming Scheme,"* CNET (Jan. 22, 2014), *available at* https://www.cnet.com/news/13-indicted-in-2m-gas-station-card-skimming-scheme/ (last viewed Feb. 3, 2017).

[9] ss. 525.01-16, F.S.; *see also* website for the Florida Department of Agriculture and Consumer Services, *Petroleum Inspection FAQ*, *available at* http://www.freshfromflorida.com/Business-Services/Petroleum-Inspection-FAQ2 (last visited Feb. 6, 2017).

[10] s. 570.65, F.S. ("Department of Agriculture and Consumer Services, law enforcement officers."); *see also* Department of Agriculture and Consumer Services website, *available at* http://www.freshfromflorida.com/Divisions-Offices/Agricultural-Law-Enforcement (last viewed Feb. 4, 2017).

[11] Harless, Linda, Department of Agriculture and Consumer Services ("DACS") Bill Analysis to HB 343 (Feb. 3, 2017) (on file with the Florida House of Representatives Criminal Justice Subcommittee).

In 2016, DACS found a total of 219 skimmers in Florida.[12] Preliminary findings for 2017 indicate that 25 skimmers were detected in January, and 9 skimmers were found in the first six days of February.[13]

State Laws Regarding Skimming

Given concerns about skimming, many states have enacted legislation to protect consumers and merchants. In 2011, the National Conference of State Legislatures ("NCSL") reported that "31 states and Puerto Rico[14] have enacted statutes that provide criminal penalties for using a credit card skimming device, also known as [a] credit card re-encoder or wedge, used to steal an individual's credit card number and data stored through the credit card's magnetic stripe."[15] Since that time, six more states have enacted anti-skimming legislation.[16] Most state laws refer to information that is encoded on the magnetic strip or stripe of a payment card. However, at least eight states[17] have included definitions or penalties to account for data encoded on computer chips or circuits,[18] which are more difficult to replicate than the information on magnetic strips.[19] "With chip cards, account numbers and expiration dates aren't actually transmitted between customer and merchant. The chips create a one-time code to fund transactions — information that would be useless to a thief trying to replicate cards."[20]

In addition, at least 13 states have laws regarding possession of a scanning device or reencoder with intent to defraud or without permission from the authorized user of the card or merchant.[21] No state, however, prevents outright ownership of such devices or creates any presumptions regarding their possession.

Currently, ch. 817, F.S., governs fraudulent practices and credit card crimes. Section 817.625, F.S., addresses the use of a "scanning device" or "reencoder" to defraud, along with their definitions.[22] Specifically:

---

[12] E-mail from Grace Lovett, Director, Office of Legislative Affairs, DACS (Feb. 6, 2017) (on file with the Florida House of Representatives Criminal Justice Subcommittee).

[13] 2017 Skimmer Deactivation List from DACS, Division of Consumer Services (Feb. 6, 2017) (on file with the Florida House of Representatives Criminal Justice Subcommittee).

[14] 33 Laws of Puerto Rico Ann. § 4863a

[15] Morton, Heather, *Credit Card Skimming Laws and Legislation, National Conference of State Legislatures* ("NCSL), *available at* http://www.ncsl.org/research/financial-services-and-commerce/credit-card-skimming-devices-laws-and-legislation.aspx (last viewed Feb. 4, 2017).

[16] The NCSL data was last updated January 24, 2011. Since that time, an additional six states have enacted anti-skimming legislation: Alabama (Ala. Code § 13A-8-113); Georgia (Ga. Code Ann., § 10-15-4); Nebraska (Neb. Rev. St. § 28-6340); North Dakota (N.D. Cent. Code, § 12.1-23-17); Tennessee (Tenn. Code Ann. § 39-14-150); and Vermont.

[17] The eight states which include language about computer chips and circuits are Alabama (Ala. Code § 13A-8-113(a)(1) and (2)); Connecticut (Conn. Gen. Stat. § 53-388a); Delaware (Del. Code Ann. tit. 11, § 903A); Kansas (Kan. Stat. Ann. § 21-6108(a)(1)-(2) and (c)(1)-(2)); Maine (Me. Rev. Stat. Ann. tit. 17-A, § 905-B(2)(C)-(D)); Minnesota (Minn. Stat. § 609.527(1)(h)-(i)); Tennessee (Tenn. Code Ann. § 39-14-150(k)(1)(A)-(B)); and Vermont (13 Ver. Stat. Ann. § 1816(a), (b), and (e)(1)-(3)).

[18] The computer chips used in payment cards are called EMV (which stands for Europay, Mastercard, Visa) cards. EMV cards "store user data on integrated circuits, or chips, that must be physically inserted into a special reader in order to be accessed." *See* Quimby, Tom, *FBI Warns New Chip Cards Insecure Among Growing Fraud*, THE WASHINGTON TIMES, Nov. 15, 2015, *available at* http://www.washingtontimes.com/news/2015/nov/15/credit-card-chip-technology-not-more-secure-than-m/ (last viewed Feb. 6, 2017).

[19] Kossman, Sienna, *8 FAQs About EMV Credit Cards, Chip? PIN? Signature? Do Old Cards Work? Answers to Frequently Asked Questions, available at* http://www.creditcards.com/credit-card-news/emv-faq-chip-cards-answers-1264.php (last viewed Feb. 6, 2017).

[20] Hardy, Kevin and Johnson, Patt, *Many Retailers Haven't Met Deadline for Chip-Card Readers*, USA TODAY (Oct. 1, 2015), *available at* http://www.usatoday.com/story/money/business/2015/10/01/chip-credit-debit-card-readers-october-1/73140516/ (last viewed Feb. 3, 2017).

[21] Ala. Code § 13A-8-113(a)(1) and (2); Ariz. Rev. Stat. Ann. § 13-2110(B); Cal. Penal Code § 502.6(a), (b), and (c); Conn. Gen. Stat. § 53-388a(f); Del. Code Ann. tit. 11, § 903A; Idaho Code § 18-2415(2); Ind. Code Ann. § 35-43-5-4.3(b)(1)-(4); Nev. Rev. Stat. § 205.606(1); N.J. Rev. Stat. § 2C:21-6.1(c); N.Y. Penal Law § 190.85; *see also* N.Y. Penal Law § 190.86 (providing that unlawful possession of a skimmer device in the first degree is a class E felony where the defendant has been previously convicted under s. 190.85 within the last five years); S.D. Cod. Laws § 22-40-14; Tenn. Code Ann. § 39-14-150(k)(2)(B); 13 Ver. State. Ann. § 1816(a)-(b).

[22] s. 817.625(1)(a) and (b), F.S.

- "Scanning device" means a scanner, reader, or any other electronic device that is used to access, read, scan, obtain, memorize, or store, temporarily or permanently, information encoded on the magnetic strip or stripe of a payment card.
- "Reencoder" means an electronic device that places encoded information from the magnetic strip or stripe of a payment card onto the magnetic strip or stripe of a different payment card.

Section 817.625, F.S.,[23] provides that it is a third degree felony[24] to use:

- A scanning device to access, read, obtain, memorize, or store, temporarily or permanently, information encoded on the magnetic strip or stripe of a payment card without the permission of the authorized user of the payment card and with the intent to defraud the authorized user, the issuer of the authorized user's payment card, or a merchant.
- A reencoder to place information encoded on the magnetic strip or stripe of a payment card onto the magnetic strip or stripe of a different card without the permission of the authorized user of the card from which the information is being reencoded and with the intent to defraud the authorized user, the issuer of the authorized user's payment card, or a merchant.

A second or subsequent violation of the statute[25] is a second degree felony.[26]

Further, any person who violates the statute is subject to Florida's civil forfeiture law.[27]

At present, there is no language in s. 817.625, F.S., regarding payment cards which are encoded with computer chips. Further, the current statute does not address possession of a scanning device, or what level of knowledge or intent is required to prove a violation, nor are there are any presumptions regarding possession or intent to defraud.

EFFECT OF BILL

The bill expands the current definitions of "reencoder" and "scanning device" to include the "computer chip" or "other storage mechanism" of a payment card. The bill further amends the definition of a "scanning device" so that it includes information encoded "from another device that directly reads the information from the payment card." The bill incorporates the amended language into the current third degree felony prohibitions against the fraudulent use of a reencoder and scanning device.

The bill also creates a new third degree felony offense that prohibits a person from possessing, selling, or delivering a scanning device knowingly and with the intent to defraud an authorized user of a payment card, the issuer of a payment card, or a merchant. For this offense, the bill specifies that it is prima facie evidence of knowledge and intent to defraud if the person possessing the scanning device is not:

- A law enforcement officer;
- An authorized representative of a law enforcement officer;
- An officer of the Department of Agriculture and Consumer Services;
- A state attorney;
- A financial security investigator employed by a merchant or financial institution;
- An authorized vendor to any of the aforementioned authorized investigative agencies; or
- A person lawfully reporting the scanning device to one of the above-listed individuals or groups.

[23] s. 817.625(2)(a), F.S.
[24] A third degree felony is punishable by up to five years imprisonment and a $5,000 fine. ss. 775.082, 775.083, and 775.084, F.S.
[25] s. 817.625(2)(b), F.S.
[26] A second degree felony is punishable by up to 15 years imprisonment and a $10,000 fine. ss. 775.082, 775.083, and 775.084, F.S.
[27] s. 817.625(2)(c), F.S. (noting, "Any person who violates subparagraph (a)1. or subparagraph (a)2. shall also be subject to the provisions of ss. 932.701-932.7062.").

The bill provides that once evidence of knowledge and intent is established, no additional identification of payment card data, payment card users, payment card issuers, or payment card merchants is required.

Finally, the bill amends the statute, incorporating the revised subsections to account for civil forfeiture.

B. SECTION DIRECTORY:

Section 1. Amends s. 817.625, F.S., relating to use of scanning device or reencoder to defraud; possession of scanning devices; penalties.

Section 2. Provides an effective date of October 1, 2017.

II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues: The bill does not appear to have any impact on state revenues.

2. Expenditures: The Criminal Justice Impact Conference ("CJIC") considered this bill on March 2, 2017. The CJIC determined that the bill will have a positive insignificant impact on prison beds, meaning an increase of ten or fewer prison beds.

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues: The bill does not appear to have any impact on local government revenues.

2. Expenditures: The bill does not appear to have any impact on local government expenditures.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR: None.

D. FISCAL COMMENTS: None.

III. COMMENTS

A. CONSTITUTIONAL ISSUES:

1. Applicability of Municipality/County Mandates Provision: This bill appears to be exempt from the requirements of Article VII, Section 18 of the Florida Constitution because it is a criminal law.

2. Other: None.

B. RULE-MAKING AUTHORITY: The bill does not appear to create a need for rulemaking or rulemaking authority.

C. DRAFTING ISSUES OR OTHER COMMENTS: As noted above, the bill provides that it is prima facie evidence of knowledge and intent to defraud for purposes of the newly created third degree felony

offense, unless the person possessing the scanning device is a law enforcement officer or other similar official. A scanning device, however, may be legitimately possessed by more people than the bill excludes, e.g., retailers, common carriers, etcetera. It may desirable to remove or otherwise amend the prima facie standard in the bill to avoid the unintended possibility of a person in legitimate possession of the device being charged with a violation of the offense.

IV. AMENDMENTS/ COMMITTEE SUBSTITUTE CHANGES

N/A